American Payroll Association
Government Relations • Washington, DC

January 19, 2007

The Honorable Alberto R. Gonzales
Attorney General of the United States

The Honorable Deborah Platt Majoras
Chair, Federal Trade Commission

Re: Identity Theft Task Force

Dear Mr. Gonzales and Ms. Majoras:

On behalf of the American Payroll Association (APA), we would like you to consider the comments below, which are being provided in response to the request for public comment issued by President George W. Bush's Identity Theft Task Force in December 2006.

About the American Payroll Association
The APA is a nonprofit professional association representing more than 22,000 individuals and their companies in the United States and Canada. The APA's central mission is to educate its members about best practices associated with paying America's workers, including compliance with all relevant federal, state, and local laws. As part of this mission, the APA works with legislative and executive branches of government to find ways for employers to meet their obligations under the law and support public policy initiatives, while minimizing administrative burden.

Many APA members volunteer their time to participate in various professional activities sponsored by the organization, including the Government Affairs Task Force – Data Privacy and Security (DP&S) Subcommittee. The primary objective of this Subcommittee is to raise awareness by educating APA members about data privacy issues like identity theft. The Subcommittee is grateful for the opportunity to provide comments.

The APA, along with other human resources groups concerned about identity theft in the employment context, such as IHRIM's Workforce Privacy Network, urges the Task Force to expand the current policy focus on consumers to include employees and the role of employers.

The APA acknowledges that identity theft is a major concern for its members and their employers and recognizes that the Task Force's recommendations will go a long way toward letting Americans know how serious the federal government is about attacking the ever-growing problem of personal data breaches and identity theft. The comments below were developed by looking through the lens of the Payroll Professional who works with sensitive employee data each day and who is acutely aware of the financial and emotional devastation caused by identity theft crimes.

I. Maintaining Security of Consumer Data

1. Government Use of SSNs

Individuals' Social Security Numbers (SSNs) should continue to be used for employee wage and tax reporting to federal, state, and local jurisdictions, as well as for the child support enforcement process. However, SSN use in any non-compliance context (e.g., as an identifying number for employees or insured's) should be limited or allowed only with safeguards in place that are enforced by government and/or employer policies and procedures.

A key safeguard is the development of a federally funded campaign to ensure awareness is embedded into the culture of every type of organization in America that the SSN and other sensitive, individual customer and employee data should be viewed as "Top Secret." The meaning of this connotation is clear. SSN data must be safeguarded using all available means!

The SSN should not be substituted with another unique identifier for government compliance purposes. Instead, the Task Force should consider recommending that the SSN be supplemented by another identifier, and the combination of the two will become a new identifier for government use. However, government forms, such as Form W-2, should continue to require only the existing nine-digit social security number rather than require all employers' payroll systems to modify this key field.

2. Comprehensive Record on Private Sector Use of SSNs

It would definitely be helpful for the Identity Theft Task Force to investigate and analyze the different ways that SSNs are used.

One option for gathering this information is to place a request to various organizations that provide support to private sector employers, like the Small Business Administration (SBA), APA, IHRIM, Society for Human Resource Management (SHRM), International Association of Privacy Professionals (IAPP), etc. The inquiry could be in the form of a survey. Sample employers could be polled as well. The survey should also be sent to employers that have publicly made known their view that privacy as a high priority. For example, contact employers that have signed up for "Safe Harbor" (http://www.export.gov/safeharbor/). Survey responses should be summarized and then published by the Identity Theft Task Force for public comments.

3. National Data Security Standards

Imposing data security standards at the national level would be helpful to employers, so long as they do not impose an unreasonable administrative burden. Such standards would clearly define minimum levels of expectations and put government agencies and private sector employers on the same level, which would in turn encourage the individual organizations to support the standards. They should also preempt state laws in this area, which would help solve a problem for multistate employers that have to comply with different, and sometimes conflicting, laws regulating data security (e.g., state laws limiting the display of employees' SSNs) in each state where they operate.

Current data security practices by employers are all over the lot. A set of national requirements would address deficiencies and reduce competitive pressure to lower costs in this area. Of course, the standards would require ongoing review and updates to keep up with advances in technology.

Data security standards should vary depending on data use no matter what size the organization is. For example, basic data security standards for electronic information (including Internet-based), hard copy records, and voice recordings should be established. Different levels of standards should be defined – from basic to advanced – for selection and use by entities (government, private sector, small business, etc.), depending on the type of data they maintain (data classification) and budget availability (employer size). Federal level incentives, such as tax credits or tax deductions, should be provided to encourage entities to establish and maintain the appropriate data security standards for their business. Data classification will identify other types of data that require lesser safeguards. A good example of why the data security standards need to vary based on data classification is the use of encryption technology (e.g., Secure Socket Layer/SSL). This technology is often used as a business best practice today when personal information that includes sensitive data like the SSN or date of birth is involved.

4. Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information

A national breach notification requirement should be adopted only if it eliminates the need to manage the requirements enacted by state and local jurisdictions. This patchwork of data breach requirements is very difficult and costly to manage.

While this section addresses "consumer information," the APA believes that the term "consumer" must be clarified. In particular, the term should include employees, and all breaches of employee data should be covered by the Breach Notice Requirements.

The essential elements of a national breach notification requirement are:

- making data breach notices available on the FTC or other central Web site and
- sending notification letters to impacted individuals.

These two simple national data breach notification standards should not vary by economic sector, business model, or business size.

If a more complex set of data breach notification standards is established, the cost of imposing them would negatively impact certain government agencies, private sector employers, and especially small business.

5. Education of the Private Sector and Consumers on Safeguarding Data

Media attention over the past few years related to data breaches and identity theft has significantly increased the awareness of safeguards that can be put into place to protect personal information. For example, based on APA member feedback, many private sector employers have converted payroll and other systems and also changed processes to limit the use of SSNs in the workplace.

Private sector employers must consider the fact that the payroll department contains a great deal of personal information like SSN, date of birth, bank account routing/account numbers, length of service, and employee name and address. The employer's data bases also probably contain personal identifying information for its employees' spouses and dependents. From the perspective of an identity thief, this group of data elements is a gold mine.

An education campaign would definitely be an appropriate way to raise awareness about the risks when a data breach occurs and the impact of identity theft. Government agencies and private sector employers have a responsibility to manage the personal information they have access to in an appropriate manner, which includes keeping it out of the hands of an identity thief. Providing context as to what constitutes legal requirements and best practices would help entities determine what they need to focus on and adhere to.

II. Preventing the Misuse of Consumer Data

The plan to develop reliable methods to authenticate the identity of an individual in a workshop setting shows promise.

There are other ways to learn about such measures as well that should be considered. In the January 7, 2007, issue of the *Atlanta Journal Constitution,* in reference to the newspaper's coverage of the identity theft problem, in the Letters section (page C8), Douglas Johnson of Albany, Ga., wrote, "Invoke a national credit freeze law that would allow consumers to block unauthorized access to their credit files and thus prevent the creation of fraudulent credit accounts. Require financial companies to use consumer-defined passwords to protect accounts, rather than easily obtained Social Security Numbers. This would cut down on pre-texting and criminal access to existing accounts."

III. Victim Recovery

1. Improving Victim Assistance

The measures being considered to provide more effective assistance to identity theft victims would certainly all be effective.

Caution is in order if measures are considered that may negatively impact employee productivity in the workplace. The government should encourage employers, through best practices efforts, to allow employees to take some time off from work to resolve identity theft issues, and employers should not be allowed to retaliate against identity theft victims for doing so. Employers should develop polices and procedures in this area as a best practice. For example, employers may wish to require employees to provide a copy of a police report and to file a formal complaint with the FTC or relevant agency for tracking purposes.

2. Making Identity Theft Victims Whole

Employers should be encouraged to prosecute an identity thief in their workplace, even if the thief is one of their own employees, by following standard processes for prosecution.

Convicted identity theft criminals should be held accountable financially for the value of time a consumer had to go through to deal with the effects of the identity theft.

The federal government should put into place appropriate standards for victim recovery awards to provide the victims some sort of compensation, but at the same time, not clog court calendars any more than they already are. This can possibly be done by providing a template for consumers to record the date, activity, and duration of their recovery efforts.

3. National Program Allowing Identity Theft Victims to Obtain an Identification Document for Authentication Purposes

APA has no comment on this section at this time.

4. Gathering Information on the Effectiveness of Victim Recovery Measures

Surveys and assessments are certainly important in providing input on the effectiveness of the program/legislation.

An evaluation of the financial impact employers and individuals (i.e. consumers, customers, contractors, employees) have incurred to comply with the required recovery measures should be obtained. For example, the data will most likely be so compelling that it will drive the cost justification for the business case for the programs the Identity Theft Task Force obtains approval to implement.

IV. Law Enforcement: Prosecuting and Punishing Identity Thieves

APA has no comment on this topic at this time.

If you have any questions or would like clarification on our comments, please contact William Dunn at the address below.

William Dunn, CPP
Manager, Government Relations
American Payroll Association
1601 18th Street, NW, Suite #1
Washington, DC 20009
Telephone: (202) 232-6889
Fax: (210) 630-4385
E-mail: wdunn@americanpayroll.org
Web site: www.americanpayroll.org

Thank you again for the opportunity to comment on this important effort.

Sincerely,

William Dunn, CPP
Manager, Government Relations

Carla G. Gracen, M.Ed., CIPP, CPP
Chair, APA Data Privacy and Security Subcommittee